Module Sixteen

Rating Maintenance Phase

This module describes all aspects of the Rating Maintenance Phase(RAMP), the final phase within NSA's Trusted Product Evaluation Program (TPEP). In particular, it addresses the responsibilities of a Vendor Security Analyst (VSA) and describes what duties must be performed by a VSA and by NSA at each stage of the RAMP process.

Module Learning Objectives

This module presents material that can be read independently of theother modules. Upon completion of this module, the student should:

1. Understand the roles and responsibilities of vendor and NSA personnel for RAMP.
2. Understand the RAMP process.
3. Understand the purpose and contents of each deliverable required for RAMP.
4. Understand what types of systems and what types of changes are allowed under RAMP.

Overview

What is RAMP? RAMP is the process by which an established rating (one given by NSA at the culmination of the Evaluation Phase) can be maintainedfor new releases of the product. In other words, future releases of the same product now have the ability to keep the original rating. RAMP begins when the Evaluated Products List (EPL) entry is published for the product at the conclusion of the Evaluation Phase. RAMP is divided into RAMP Cycles, where a RAMP Cycle is the period of time between two consecutive EPL entries for a product.

This module begins by describing the roles and responsibilities of each of the individuals involved in RAMP, including the training needed to participate in RAMP. Then, the activities and deliverables involved in RAMP are described. The module concludes with a discussion of what kinds of changes are allowed under RAMP.

RAMP Roles and Responsibilities

To understand the way RAMP works, each of the NSA and vendor individuals must be identified and their corresponding roles and responsibilitiesdiscussed. The important representatives from NSA are the Project Manager and the Technical Point of Contact (TPOC). Each vendor has corresponding positions for interfacing with NSA and providing management oversight and technical direction: the Responsible Corporate Officer (RCO) and the VSA.

Project Manager

The Project Manager is NSA's business representative who is responsible for overseeing NSA's portion of the TPEP process. This person is responsible for all TPEP phases (Pre-Evaluation, Evaluation, and RAMP, as described in Module

4). The Project Manager is always an NSA employee. All business questions and concerns should be addressed to the appropriate Project Manager.

Technical Point of Contact

The TPOC is NSA's technical representative who is a member (or members) of the NSA evaluation community. This community is comprised of NSA evaluators and evaluators from several Federally Funded Research and Development Centers (FFRDCs), such as the MITRE Corporation, the Institute for Defense Analyses, and the Aerospace Corporation. During the evaluation of a product, the evaluation team serves as the TPOC. The evaluation team reviews the Rating Maintenance Plan (RM-Plan) andanswers all RAMP-related questions. Prior to the Final Technical Review Board (TRB), a single person is identified as the RAMP TPOC. For purposes of continuity, every effort is made to ensure that a member of the original evaluationteam continues with the product through RAMP. This person's role begins after completion of the Final TRB and continues throughout the RAMP lifetime of the product. The TPOC's role in the RAMP process is to provide guidance and answer technical questions posed by the vendor, to keep the VSA appraised of potential changes to the TCSEC, and to conduct audits of the vendor's RAMP Evidence. The TPOC also coordinates the review of any documents submitted as evidence of sustained system trust, and schedules a RAMP TRB, upon the VSA's request, when the supporting evidence is sufficient to warrant the continuation of the rating with the new system release.

Responsible Corporate Officer

The RCO is the vendor's business representative who is responsible for the continued trust of the product. The RCO must have sufficient management responsibility and authority over the product being evaluated to ensurethat its rating is maintained during its continued development and maintenance. The RCO may delegate specific RAMP responsibilities to a Vendor Business Point of Contact (VBPOC). The RCO supports the VSA so that the productmaintains its rating. The VSA must have the necessary tools to maintain the rating and have the ability to influence change decisions such that no change adversely impacts the security rating of the system. If a VSA is unable to prevailin a situation in which a change will adversely impact the continued trust of the product, the RCO must be in a position to veto the change to the product. Security must dominate all other requirements such that the modification or implementation of features does not compromise the security of thesystem. The RCO provides a level of management above the VSA that understandsthe role of the VSA, and has enough influence in the company to assure thatthe VSA will be able to properly perform his duties.

Vendor Security Analyst

The VSA is the vendor's technical representative. A vendor using multiple VSAs must designate a lead VSA to provide a single point of contactbetween the vendor and NSA. The VSA (or team of VSAs) provides theequivalent function of the vendor's original evaluation team, applying TCSEC expertise during the evaluated product's continued development and maintenance.

The primary responsibility of VSA(s) is the collection,documentation, and presentation of the evidence of continued trust in their product. As a fundamental element of this responsibility, at least one VSA is expected to review each change to the product based on the assessed security relevance of the change. The VSA will likely contribute to writing the RM-Plan, which outlines the methods employed by the vendor to ensure continued product trust. To ensure continued compliance with the TCSEC, VSAs must keep abreast of changes to the TCSEC through Interpretations or the issuance of a new version of the TCSEC. In order to be aware of any TCSEC changes, the VSA must be familiar with, and routinely access, the computer system NSA uses for interaction with the security community, called Dockmaster.

Since the VSA must know the TCSEC, NSA provides the RAMP training to educate VSAs. Only NSA-recognized VSAs (personnel that have completed the NSA-sponsored course of training) can represent their product to NSA.Every product being evaluated or currently under RAMP must have at least one NSA recognized VSA. To be a recognized VSA, a person must successfully complete both the non-resident portion of the RAMP training course (containedin this set of materials) and the resident portion, which is offered when sufficient demand warrants. The minimum expectation is that the VSA understand the security implications of a change and be able to present that understanding at the RAMP TRB, where senior evaluators can review the security analysis and the decisions made. With each interaction with NSA, the VSA's technical credibility becomes clearer. If NSA feels that a vendor's product may be in jeopardy of losing its rating because of perceived inability of itsVSA(s), NSA will inform the RCO of the potential problem.

RAMP Activities

At this point, the reader should be able to identify the four majorindividuals involved in RAMP and identify their roles and responsibilities. This section describes the generic activities that take place during RAMP: system identification, security analysis, collecting RAMP Evidence, and conducting RAMP Audits. Each of these activities is to be customized by vendors for their particular environment and captured in their RM-Plan. A typical RAMP maintenance action is presented at the end of this section.

System Identification

Systems are identified by decomposing the system into smaller subsets, or configuration items (CIs), and then naming each item. For RAMP, the granularity of a CI must be sufficient to support the securityanalysis of future changes. At C2 and B1, the TCB, the integrity validation features, the informal or formal model of the security policy (at B1), the SFUG, the TFM, the test plan and procedures that show how the security mechanisms were tested, the expected results of the security mechanisms' functional testing, the design documentation, and the RM-Plan must be described in terms of CIs. At B2 and above, the Configuration Management Plan (CM-Plan) must also be a CI. Initial Product Assessment Report (IPAR) and Final Evaluation Report (FER) appendices identify the evaluated hardware and software configuration for a product. These CIs can be used as a starting point for systemidentification.

Security Analysis

RAMP exists because systems change. To maintain the rating of a system, NSA needs to know what changes have taken place from one version of a system to the next. In addition to knowing what changes have been made to a system, NSA needs to know that those changes have not adversely affected the security mechanisms and assurances of the system. Security analysis is closely coupled with the configuration management activities, in that every change must be analyzed with respect to its effect on all elements of the TCB. The analysis must take into account the side effects of changes (interrelationships between components of the TCB) and the cumulative effects of multiple changes to the components.

Security analysis is an examination of the TCB to determine whether agiven change, or set of changes, upholds the security features and assurances of the original evaluated product. The RM-Plan outlines the vendor's policies and procedures for security analysis. All components of the system must be identified, and baselined, at the beginning of the Evaluation Phase. In order to RAMP future releases of the product, each ensuing change to the baseline system must be approved and take place under the configurationmanagement procedures described in the RM-Plan.

The most important function of security analysis is to ensure that no changes are made to the system that will adversely affect the security. At C2 and B1, security analysis is performed by the VSA(s); at B2 and above, it is performed by a Security Analysis Team (SA-Team). The VSA(s)/SA-Team will have to show NSA that any changes to the TCB still uphold the security mechanisms and assurances of the system and have no negative impact on the system for meeting the TCSEC requirements. Because all changes must be approved and a determination made concerning the effects of a change on the security of the system, at least one VSA/SA-Team member must perform security analysis on each change.

For RAMP, an approved set of procedures for managing changes must be available, understood, and followed. These procedures should be clearly explained in the RM-Plan to include how the implementation of changes are proposed, evaluated, coordinated, and approved or disapproved. TheRM-Plan must also include the steps taken to ensure that only the approved changes are actually implemented and that all tests and documentation needed to show compliance with the TCSEC are consistently updated.

There are two methods for managing changes to a system: control and review. Control requires that a proposed change be analyzed before it is implemented. Review analyzes the effects of changes after they are implemented but before they are integrated into the system. C2 and B1 systems require designreview and testing, a post-analysis activity. B2 and above products require control to be enforced through a Future Change Review Board (FCRB). Althoughit is desirable and expedient to determine the effects of changes before they are implemented and to manage those changes from the very outset, control is not required for C2 and B1 products participating in RAMP. However, unnecessary development efforts could be avoided by conducting the security analysis on proposed changes as part of a control process. As a result, NSA has allowed vendors of C2 and B1 products to appear before an FCRB to discussproposed changes to the product under RAMP; NSA may also allow an SA-Team to be formed and provide NSA resources to perform the security analysis relatedto those changes.

RAMP Evidence

RAMP Evidence is the vendor's record of security analysis. It provides a record of the information needed to manage a configuration effectively andprovides the status of proposed and approved changes. Specifically, for each change, RAMP Evidence includes: a description of the change; the issues and conclusions of the security analysis; what CIs were affected; and the statusof the changes to the CIs (e.g., being implemented, or completed). The extent of these efforts will be impacted by whether the system is subject to justreview or also control.

RAMP Audits

A RAMP Audit consists of checks by the vendor to determine the consistency and completeness of its configuration accounting information. The RAMP Audit is designed to test the process to show that the trail of RAMPEvidence is truly being captured and to check the validity of the evidence being captured. Because security analysis and RAMP Evidence are the keys to success in RAMP, vendors should periodically perform RAMP Audits to verify that the configuration accounting information is accurate and complete. A VSA-conducted RAMP Audit is required to be performed at least once per RAMP Cycle. Similarly, an NSA-conducted RAMP Audit is required to be performed once per RAMP Cycle.

Typical RAMP Maintenance Action

For each new product release under RAMP (i.e., for each RAMP Cycle), the RCO must submit a package to NSA. This package must contain the RM-Plan, an updated FER, a new product description proposed for entry on the EPL,and a new Rating Maintenance Report (RMR). The following modelhighlights the events surrounding a typical RAMP Action (note that "VSA" should be replaced with "SA-Team" for B2 and above products):

1. FCRB reviews proposed changes. (B2 and above only)
2. VSA(s) performs security analysis and archives RAMP Evidence.
3. Vendor develops required RAMP deliverables.
4. Vendor submits package to TPOC.
5. TPOC forwards package to TRB members and schedules TRB.
6. TPOC notifies VSA of date, time and location of RAMP TRB.
7. TRB prepares comments, criticisms, and questions that are forwarded to the VSA.
8. TRB members, TPOC, other evaluators, and VSA(s) participate in the RAMP TRB meeting. The RCO is invited to attend.

9. The VSA(s) presents the contents of the RMR and discusses any questions or concerns raised by the TRB and evaluation community.
10. Upon completion of the presentation, the TRB caucuses.
11. VSA(s) and TPOC are then brought back in and informed of the TRB's recommendations (the TRB is an advisory panel only, they do not make decisions).
12. TRB recommendations are forwarded to Chief of Product Evaluations.
13. Chief of Product Evaluations makes decision of acceptability of product trust (may differ from TRB recommendations).

The TRB is NSA's quality assurance group. The TRB serves as a checkpoint for the quality, uniformity, and consistency of evaluation. The TRB adds a quality assurance step to the evaluation process to ensure that all products are evaluated fairly and equitably against the same criteria.

RAMP Deliverables

Having examined the generic activities that take place during RAMP, this section describes the deliverables that must be submitted by the vendorfor a RAMP Action. Besides updating the existing FER and EPL entry toreflect implemented changes, the vendor must produce a new RMR and also must submit a copy of the NSA-approved RM-Plan for the product.

Rating Maintenance Plan

An RM-Plan is a plan for rating maintenance activity that must beproduced by the vendor for each product participating in RAMP. NSA requires an RM-Plan because it realizes that each vendor does business slightly differently. Rather than dictate methods that undoubtedly would not match a vendor's current method of developing and maintaining systems, the RM-Plan allows the vendor to customize RAMP to a particular work environment. It is recommended that the initial RM-Plan reflect the vendor's current method of doing business. It is conceivable that the current methods are sufficient for RAMP. If not, the evaluation team or the TPOC will work with the vendor to resolve any deficiencies to the mutual satisfaction of both. Ideally, RAMP should have little or no impact on the methods a vendor employs to develop and maintain its product.

The RM-Plan is developed with guidance from NSA, and it ultimately mustbe approved by NSA. The RM-Plan describes the procedures that will be usedto ensure that the security mechanisms and the assurances of the product are properly maintained. It must provide a rationale for systemidentification along with a list of CIs, must describe how security analysis and RAMP Audits will be carried out, and must delineate how RAMP Evidence will berecorded and maintained. If a failure occurs in the RAMP process, the RM-Plan must be updated to reflect the corrective measures that were taken. Since each vendor is likely to implement RAMP differently, NSA will be judging the RM-Plan on completeness and feasibility.

The RM-Plan must show that the described mechanisms, procedures, and tools are sufficient to address all changes to the product. In particular, the vendor's approach to distributing bug fixes and new features must be explained. The discussion on bug fixes must distinguish between emergency fixes forsevere security vulnerabilities and routine fixes for minor security andnon-security bugs. The vendor should notify the TPOC immediately about any bug fixesthat could be sent out to users on an emergency basis. This notification avoids confusion when customers call NSA to ask about a specific bug fix.

The RM-Plan should identify the frequency of releases of the trustedproduct. NSA wants to keep the evaluated products list manageable, and the vendors do not want to continue to maintain older versions of a system forever. Therefore, the plan also needs to highlight a schedule or specific plan for the retirement of older versions of the system.

A portion of the RM-Plan must address how the vendor intends toincorporate current and future changes or Interpretations to the TCSEC in a timely manner. At a minimum, the vendor should expect to do something like the following:

- VSAs will review the **`Announce`** meeting on Dockmaster weekly looking for Interpretations.
- publication of a proposed Interpretation will result in a corporatecaucus to assess the impact on the system.
- a plan of action will be formulated to address the Interpretation.
- the VSA will inform the TPOC of the expected compliance schedule.

To keep track of pending changes to the TCSEC, VSAs should participate in the discussions on the **`Criteria-Discussions`** meeting. These "open debates" allow the VSA to voice specific concerns or opinions aboutInterpretations of currently contentious requirements of the TCSEC. Through participation in the forum, the VSA can influence the content of the Interpretation, orat the very least have advanced warning of pending Interpretations.

During the life of a product, the RM-Plan may need to be revised. The RM-Plan must include a section that describes the procedures used to make changes to the plan. Since changing the RM-Plan changes the potential assurance implied by the approved process, proposed changes must be submitted for review by NSA. Failure to propose these changes to NSA before implementation or failure to consider comments returned by NSA may result in a change in the product that will not be acceptable during the review process. The RM-Plan must include the original data of its approval and the dates of all approved changes. It is emphasized that an NSA-approved RM-Plan must always be in effect for RAMP to continue.

The last, though certainly not least, topic for the RM-Plan concerns the description of the organizational framework within the company todevelop and support the trusted product. Critical in this description is the identification of the VSA(s) and the RCO within that organizationalong with their roles and responsibilities. If there are multiple VSAs, the division of responsibilities between them must be identified. One VSA for each product must be designated as the lead VSA, providing a single point of contact between the vendor and NSA. The lead VSA need not have supervisory responsibility over other VSAs.

In summary, the RM-Plan is a detailed description of the RAMP process the vendor plans to implement. NSA will review and, if it is found adequate, approve the plan for implementation. NSA approval implies the process is necessary and sufficient to gather and present the information neededto maintain the trust of the product. If the plan is followed, the vendorwill ha ve all the information NSA needs to determine whether or not a given releasehas maintained its rating. The RM-Plan is part of the evidence evaluated during the evaluation of the product. The RAMP process shall be in operationprior to the completion of the Evaluation Phase. In this way, ongoing changes and development efforts for future releases will be properly analyzed and thetrail of evidence developed, sustaining trust in each ensuing release. It also gives the vendor the opportunity to “debug” their RAMP process beforeproceeding on their own.

Rating Maintenance Report

The RMR is presented to the TRB as a summary of all RAMP Evidence generated during a particular RAMP Cycle. There are different levels of change which require different amounts of detail in the RMR; non-TCB changes must simply be identified, non-security-relevant TCB changes must be given justification as to their non-security relevance, and security-relevant TCB changes must be described in detail. The RMR must also address any new TCSEC Interpretations that are applicable.

Changes Allowed Under RAMP

The most frequent question of those involved in RAMP is, “What changes or updates are allowed under RAMP?” This, unfortunately, is a difficult question to answer. What is allowed under RAMP for one product may not be allowed for another product. A change must be analyzed in the context of the specifics of the system in question. Acceptability of RAMP changes cannot yet be determined out of context (i.e., vague generalities). There is, however, some general guidance that can be offered. First, there are degrees of acceptability. In other words, it is a gray scale that must take into account the effects of the change on the TCB of the product. For example, changes in a particular feature in one system may not effect the trust of the system because there were no trust requirements allocated to the module, while the same feature change in another system with a different architecture may need to be scrutinized very carefully. Second, acceptability of RAMP changes is cumulative (i.e., it is compared against the original evaluated product to determine degree of change). Once a product has passed a certain point in its evolution,NSA ma y determine that the product can no longer be maintained through RAMP, and thus require that the product be submitted for a new evaluation.

Software modifications that dramatically change the fundamental access control mechanism are likely candidates for re-evaluation by NSA. Acceptability of hardware changes under RAMP is usually a function of compatibility with previous hardware. For example, a system that uses an Intel

80286 CPU and migrates to the upwardly compatible Intel 80386 can expect to RAMP if done properly. A vendor using the Intel 80286 cannot, on the other hand, expect to migrate to the Motorola 68030. This type of change would require substantial rework to the underlying architecture of the trusted system.

TPOCs are responsible for helping vendors understand what is, and is not, allowed under RAMP for their particular system. If a certain set of changes is not allowed, the vendor may request a re-evaluation in a timely manner. Because of the ongoing analysis and documentation of product trust under RAMP, the requested re-evaluation should go smoothly.

Relevant Trusted Product Evaluation Questionnaire Questions

None.

Required Readings

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria,* DoD 5200.28-STD, December 1985.

The RAMP requirements are in [RAMP94]. Sections 2.1.3.2, 2.2.3.2, 3.1.3.2, 3.2.3.2, 3.3.3.2, 4.1.3.2, 5.3.3, 7.5 and 10.0, and Appendix D discuss life-cycle assurance. Note that not all of RAMP requirements for the trusted product life-cycle are mentioned in the TCSEC. Note also that some of the B2 and above TCSEC requirements are required for any product participating in RAMP.

RAMP94 National Computer Security Center, *Rating Maintenance Phase: Program Document*, Draft, Version 2, 1 March 1994.

This document contains the list of RAMP requirements for classes C2-A1. It has the format of definitions followed by requirements. The information in this document supersedes the information in [RAMP89].

Supplemental Readings

CM88 National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems*, NCSC-TG-006, Version 1, 28 March 1988.

While the guideline concentrates on configuration management (CM) for TCSEC classes B2 through A1, much of the material is pertinent to lower assurance classes. Although this guide does not cover CM for systems under RAMP, it is useful in describing typical CM processes and tools that can be used in RAMP.

RAMP89 National Computer Security Center, *Rating Maintenance Phase: Program Document*, NCSC-TG-013, Version 1, 23 June 1989.

This document originally defined the RAMP process, products, roles and responsibilities. It contains an example of how the

RAMP requirements may be met and contains further insight into the history of and meaning of RAMP. This document has evolved into [RAMP94].

Other Readings

Boehm88 Boehm, B.W., “A Spiral Model of Software Development and Enhancement,” *IEEE Computer*, Vol. 21, No. 5, pp. 61-72, May 1988.

Crocker89 Crocker, S.D and Siarkiewicz, E.J., “Software Methodology for Development of a Trusted Battle Management System: Identification of Critical Problems,” *Proceedings of the 5th Annual Computer Security Applications Conference*, pp. 148-165, December 1989.

Marmor89 Marmor-Squires A. et al., “A Risk-Driven Process Model for the Development of Trusted Systems,” *Proceedings of the 5th Annual Computer Security Applications Conference*, pp. 184-192, December 1989.

Pozzo84 Pozzo, M.M., “Life Cycle Assurance for Trusted Computer Systems: A Configuration Management Strategy for Multics,” *Proceedings of the 7th DOD/NBS Computer Security Conference*, pp. 169-179, September 1984.